TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 28th of December to 03rd of January, 2026
Report No.: TZ-CERT/WRHP/2026/52

1. NETWORK ATTACKS

A total of **818,737** attacks have been recorded compared to last week's **517,365** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords are as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	78.111.67.73	root	123456
2.	45.179.216.18	admin	password
3.	185.11.61.226	zabbix	admin
4.	91.92.241.148	tomcat	qwerty
5.	185.11.61.151	solana	P@ssw0rd
6.	204.76.203.83	rafael	12345678
7.	193.105.134.95	oracle	root123
8.	185.246.128.133	ubuntu	P@ssw0rd123
9.	157.245.66.5	steam	(empty)
10.	176.65.132.95	apache	123456789

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and passwords be made to avoid use of the above listed credentials and default ones. The use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **406,178** malicious software distributed, compared to last week in which was **359,900.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Trojan:Linux/Multiverze!rfn	aa85190274311673a61039d434c6b30a0f694ce645a0340f0c11424d0eff8f87
2.	41.59.201.132	Miner:Linux/CoinMiner.99dbe0da	0291de841b47fe19557c2c999ae131cd571eb61782a109b9ef5b4a4944b6e76d
3.	41.59.203.60	Linux/CoinMiner.ABF Trojan	243407432245afff15e8c3aeb3422eb878c53acd2b0f9468c47d613a4f652abe

4.	222.73.230.171	HEUR:Trojan.Linux.Miner.gen	2ea782041e1edf52de42fdb415c63b4e2d0a24e3801385611d4c668c708a6457
5.	207.148.35.106	Trojan.Script.Multiverze.4!c	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
6.	41.59.201.7	Adware.Linux.GenericKD.22	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
7.	41.139.177.151	Malware.LINUX/AVI.Agent.cciiu	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
8.	90.154.127.19	BASH/Mirai.AEH!tr.dldr	a4937335be62e9843f12854b43ea2ac007e27863aeb3d36c418cc09d63b49642
9.	196.190.84.202	HTML.ExploitKit	40bec1ee86a5ba5ed620bbe546b09d072481d71356ba2025974c08a0e3f3fb0c
10.	41.59.211.41	Trojan:JS/Berbew	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **21,616** web attacks compared to last week which was **9,453.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 28th of December to 03rd of January, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	35.180.79.191	/
2.	38.58.182.203	/robots.txt
3.	193.243.147.243	/favicon.ico
4.	109.130.169.112	/.env
5.	195.178.110.192	////admin/config.php
6.	138.197.114.112	/SDK/webLanguage

7.	143.198.147.197	/sitemap.xml
8.	195.178.110.204	/.well-known/security.txt
9.	204.76.203.212	////search
10.	78.153.140.151	/.git/config

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,078** ICS attacks compared to last week which was **4,597.**

From the table below these are the top 5 ICS attacks and their associated attacking IP, exploited protocols and exploited ports as detailed for the period between 28th of December to 03rd of January, 2026, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	109.130.169.112	kamstrup_protocol	1025
2.	77.83.240.70	IEC104	2404
3.	35.180.79.191	guardian_ast	10001
4.	3.137.73.221	kamstrup_management_protocol	50100
5.	3.149.59.26	snmp	161

Table4: Top 5 ICS attacking IP

5. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with the most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

5.1 Note that most of the malicious IP addresses captured are also listed as malicious IP addresses in other sources that are also observing security attacks; thus, security measures should be considered to counteract, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.

5.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

5.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.

5.4 Deploy Intrusion Detection System (IDS) and configure it to flag the detection of attacks associated with the list of resources provided especially the IP addresses and the web requests.